



# Department of Homeland Security Daily Open Source Infrastructure Report for 28 February 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The New York Times reports that among global cybercriminals phishing may already be passe, being eclipsed by keylogging software that can infect computers, silently copy the keystrokes of their users, and send that information to the crooks. (See item [15](#))
- Federal Computer Week reports the recent response after Hurricane Katrina has highlighted the need to standardize digital maps using Global Positioning System devices and print-on-demand maps, navigation aids that were unavailable even a decade ago. (See item [40](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *February 27, Business First of Buffalo (NY)* — **National Grid to buy KeySpan.** National Grid is going through with a deal to buy KeySpan Corp. for \$7.3 billion the energy companies announced Monday, February 27. Terms call for National Grid to acquire KeySpan, based in New York City. National Grid operates the former Niagara Mohawk Power Corp., serving some two million electric and gas customers in upstate New York. National Grid, based in London, has additional operations in the Northeast as National Grid USA. When completed, officials said it will create the third-largest energy delivery utility in the U.S., with electricity

and gas businesses serving nearly eight million customers in the New York State and New England regions. KeySpan will become a wholly owned subsidiary of National Grid and will continue to operate as KeySpan.

Source: [http://www.bizjournals.com/industries/energy/electric\\_utilities/2006/02/27/buffalo\\_daily1.html](http://www.bizjournals.com/industries/energy/electric_utilities/2006/02/27/buffalo_daily1.html)

2. *February 27, Federal Computer Week* — **Energy launches mega search effort.** A year from now, Internet users will be able retrieve scientific research from four major portals — Science.gov, a portal with millions of pages of pre-publication research findings, a search engine for science conference proceedings, and a database of international research on energy — by entering one query on one Website. The mega portal initiative, dubbed Global Discovery, is a program of the Energy Department's Office of Scientific and Technical Information (OSTI). OSTI has operated Science.gov since 2002, which offers one-stop access to PubMed, MedlinePlus, and DefenseLINK, among other databases. Analysts estimate that the majority of Web-accessible scientific documents are in databases, inaccessible to traditional search engines. Global Discovery's goal is to accelerate scientific advancement by diffusing new research.

Source: <http://www.fcw.com/article92415-02-24-06-Web>

3. *February 25, Associated Press* — **Al Qaeda claims attack on Saudi refinery.** Suicide bombers carried out an attack on the world's largest oil processing facility Friday, February 24 but were stopped from breaking in by guards. Al Qaeda purportedly claimed responsibility for the attack, the first on an oil facility in Saudi Arabia. The assault raised speculation that the militants were adopting the tactics of insurgents across the border in Iraq, where the oil industry has been repeatedly targeted. Saudi Oil Minister Ali Naimi quickly announced that the attack "did not affect operations" and that Abqaiq operations and exports "continued to operate normally." The huge Abqaiq processing facility near the Persian Gulf prepares about two-thirds of the country's oil output for export, making it a crucial link in getting Saudi crude to the market. Crude oil futures spiked more than \$2 a barrel amid fears militants would again target the vital industry. There have long been fears militants would target oil facilities, but in the past they have targeted foreigners working in the industry rather than infrastructure.

Source: [http://news.yahoo.com/s/ap/20060225/ap\\_on\\_re\\_mi\\_ea/saudi\\_explosion\\_44](http://news.yahoo.com/s/ap/20060225/ap_on_re_mi_ea/saudi_explosion_44)

4. *February 25, Chicago Tribune (IL)* — **Exelon reports minor problem at Byron plant; fourth problem in week at a nuclear reactor.** Another problem struck an Exelon Corp. nuclear plant when electrical equipment Friday, February 24 unexpectedly began giving off smoke at the Byron Generating Station, located about 90 miles west of Chicago, IL. Although relatively minor, the incident was at least the fourth problem to hit an Exelon nuclear plant since Monday, February 20. Operators at Byron declared "an unusual event," the lowest of four federal emergency classifications, at 8:54 a.m. CST after smoke was found in a room connecting two buildings at the Byron Unit 1 reactor. Exelon said that there were no injuries and no release of radiation, and that the plant continued to operate normally. Nesbit said electrical problems outside the plant caused the reactor to shut down automatically as a protective measure. Exelon and the Nuclear Regulatory Commission are investigating.

Source: <http://www.chicagotribune.com/business/chi-0602250165feb25.1.6691242.story?track=rss>

5. *February 24, Associated Press* — **Problem halts Tennessee uranium tank project.**

Reinforcing steel was missing or not installed as designed in some concrete walls and floors in a \$350 million storehouse that will hold the nation's largest inventory of bomb-grade uranium, according to federal inspectors. The National Nuclear Security Administration could not say how significant the problems were at the construction site within the Y-12 nuclear weapons complex in Oak Ridge, TN. The discovery has forced suspension of most work on the new uranium facility since Friday, February 3, according to the Defense Nuclear Facilities Safety Board. The construction problems raise questions about the structural integrity of a building to store a dangerous cache that lies within a region of periodic but mild earthquake activity. The Y-12 plant makes parts for every warhead in the country's nuclear weapons arsenal.

Source: [http://news.yahoo.com/s/ap/20060225/ap\\_on\\_re\\_us/uranium\\_storehouse\\_1](http://news.yahoo.com/s/ap/20060225/ap_on_re_us/uranium_storehouse_1)

6. *February 24, Reuters* — **Oregon approves sale of PacifiCorp utility.** The State of Oregon on Friday, February 24 approved the sale of utility PacifiCorp to MidAmerican Energy Holding Co. for \$9.4 billion, becoming the last of six states that need to approve the sale, the Oregon Public Utility Commission said. The sale had already been approved by utility commissions in the other five states served by PacifiCorp — Idaho, Utah, Washington, Wyoming, and California. PacifiCorp has 1.6 million customers in the six states. It operates as Pacific Power & Light Co. in Oregon, Washington, Wyoming, and California, and as Utah Power in Utah and Idaho. The Federal Energy Regulatory Commission, the Nuclear Regulatory Commission, and the U.S. Department of Justice also have approved the sale.

Source: [http://news.yahoo.com/s/nm/20060224/bs\\_nm/utilities\\_pacificorp\\_acquisition\\_dc\\_1](http://news.yahoo.com/s/nm/20060224/bs_nm/utilities_pacificorp_acquisition_dc_1)

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

7. *February 27, Daily Times–Call (CO)* — **Chemical plant fire in Colorado prompts**

**evacuation.** A fire at a Fort Lupton, CO-area oil and gas plant injured a contract employee and created a tower of black smoke visible from as far as 40 miles away, according to emergency officials. Doug Houk, spokesperson for EnCana Oil & Gas, said the fire started at about noon in a compressor station at the facility. Using a reverse-911 system, emergency officials asked residents from about 90 surrounding homes in a four-mile radius to evacuate the area while firefighters worked on dousing the blaze at the plant.

Source: <http://www.longmontfyi.com/Local-Story.asp?id=6418>

8. *February 27, Contra Costa Times (CA)* — **Diesel spill slows interstate traffic in California.**

An early morning big rig crash Monday, February 27, in the Altamont Pass spilled diesel fuel and snarled morning traffic along Interstate-580, the California Highway Patrol said. About 75 gallons spilled from a rupture in the big rig's 100-gallon tank.

Source: <http://www.contracostatimes.com/mld/cctimes/13974010.htm>

9. *February 26, Midland Daily News (MI)* — **Chemical fire prompts road closure in Michigan.**

An early morning fire Saturday, February 25, at Dow Corning Corp.'s Saginaw Road facility in Midland, MI, closed the Salzburg, Saginaw, Waldo and Bay City roads. The leak was caused by a chlorosilane-based material. Downwind air monitors did not detect chemicals escaping the

plant.

Source: [http://www.ourmidland.com/site/news.cfm?newsid=16200908&BRD=2289&PAG=461&dept\\_id=472542&rfti=6](http://www.ourmidland.com/site/news.cfm?newsid=16200908&BRD=2289&PAG=461&dept_id=472542&rfti=6)

10. *February 26, KHOU (TX)* — **Unknown chemical spills into Texas creek.** Officials said what appeared to be a blue chemical spilled over the course of five miles in Crystal Creek, east of Conroe, TX, in Montgomery County on Sunday, February 26. Although not yet identified, officials believe the substance is a harmless dye.  
Source: [http://www.khou.com/news/local/montgomery/stories/khou060226\\_ac\\_chemicalspill.665d2032.html](http://www.khou.com/news/local/montgomery/stories/khou060226_ac_chemicalspill.665d2032.html)
11. *February 26, State (SC)* — **South Carolina railroad yard evacuated due to chemical leak.** A CSX railroad yard off in Cayce, SC, was evacuated for several hours early Sunday morning, February 26, after a toxic chemical, Alkyl Phenol, leaked from a train car and mixed with rain, causing a small cloud to form, according to Charles McNair, director of Cayce's Department of Public Safety. McNair said once airborne, the chemical has a 700 foot radius, so public safety officials set up a perimeter to keep people away.  
Source: <http://www.thestate.com/mld/thestate/news/local/13968392.htm>
12. *February 23, Chicago Sun–Times* — **Boiler causes carbon monoxide leak in apartment building; 50 evacuated.** The owner of an apartment building where a carbon monoxide leak forced the evacuation of about 50 people Wednesday night, February 22, had repairs made to a boiler Thursday, February 23. Residents of the building were not allowed to return until Friday, February 24, to allow the owner time to install carbon monoxide detectors in all units and make sure smoke detectors were working properly.  
Source: <http://www.suntimes.com/output/news/carbonmon23.html>
13. *January 27, Government Accountability Office* — **GAO–06–150: Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed (Report).** Terrorist attacks on U.S. chemical facilities could damage public health and the economy. While the Environmental Protection Agency (EPA) formerly led federal efforts to ensure chemical facility security, the Department of Homeland Security (DHS) is now the lead federal agency coordinating efforts to protect these facilities from terrorist attacks. The Government Accountability Office (GAO) reviewed (1) DHS' actions to develop a strategy to protect the chemical industry, (2) DHS' actions to assist in the industry's security efforts and coordinate with EPA, (3) industry security initiatives and challenges, and (4) DHS's authorities and whether additional legislation is needed to ensure chemical plant security. GAO interviewed DHS, EPA, and industry officials, among others. GAO recommends that (1) Congress consider giving DHS the authority to require the chemical industry to address plant security, (2) DHS complete the chemical sector–specific plan in a timely manner, and (3) DHS work with EPA to study the security benefits to plants of using safer technologies. After reviewing a draft of this report, DHS agreed in substance with GAO's first two recommendations but expressed concerns about studying safer technologies. GAO continues to see merit in such a study. EPA had no comments on the draft report.  
Highlights: <http://www.gao.gov/highlights/d06150high.pdf>  
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-150>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

14. *February 27, National Defense* — **Urban battlefield is proving ground for unmanned aerial systems.** Unpiloted aircraft are proliferating in war zones in Iraq and Afghanistan. But while the demand for smaller and more capable systems continues to grow, analysts say that in order to make these aircraft more effective in the urban environment, a fistful of technology improvements are needed. In the open battlefield environment of past conflicts, small numbers of Unmanned Aerial Vehicles (UAVs) were typically used for reconnaissance missions. Now that the fight has moved into city streets, unmanned systems have encountered some challenges. Buildings can block the line-of-sight of an aircraft and interfere with its communications and flight operations. "We need to close that identification-engagement gap," says Russell Glenn, senior defense analyst with RAND Corp. The enemy has learned how to exploit that weakness by simply ducking into buildings and challenging rules of engagement, says Glenn. In addition, the transmission of video and imagery on limited bandwidth is causing difficulties. Information from UAVs often traverses a number of channels before reaching a decision maker. "Ideally, what you would have is every system being able to communicate with every data transmission system, such that UAV 'A' would be able to provide information directly, rather than having to go through nodes," says Glenn.

Source: [http://www.nationaldefensemagazine.org/issues/2006/march/urban\\_battle.htm](http://www.nationaldefensemagazine.org/issues/2006/march/urban_battle.htm)

[\[Return to top\]](#)

## **Banking and Finance Sector**

15. *February 27, New York Times* — **Keylogging gaining popularity; phishing may already be passe.** Evidence exists that among global cybercriminals phishing may already be passe. In some countries, it's been eclipsed by an even more virulent form of electronic con — the use of simple keylogging software that can infect computers, silently copy the keystrokes of their users and send that information to the crooks. "It's the wave of the future," said Peter Cassidy of the Anti-Phishing Working Group. Keylogging's simplicity may be why it is suddenly so popular among some thieves. "Phishing takes a lot of time and effort... This type of software is a much more efficient way to get what they're after," said David Thomas of the FBI. The programming, too, is often trivial. Said Eugene Kaspersky of Kaspersky Labs: "These can be developed by a 12-year-old hacker... I'm afraid that if the number of criminals grows with this same speed, the antivirus companies will not be able to create adequate protection." He added that the time has come for increased investment in — and far better cross-border cooperation between — law enforcement agencies.

Source: [http://news.com.com/Cyberthieves+silently+copy+keystrokes/2100-7349\\_3-6043433.html?tag=cd.top](http://news.com.com/Cyberthieves+silently+copy+keystrokes/2100-7349_3-6043433.html?tag=cd.top)

16. *February 27, Newsday (NY)* — **Spammers exploiting social networking Websites.** Spammers are trying a new way to trick Internet users into handing over personal information by posing as a friend. Exploiting social networking Websites like myspace.com and facebook.com,

spammers and identity thieves are making junk e-mail look like it was sent by the recipient's friend, cyber-crime experts say. Although the practice of sending e-mails from fake corporate Websites, known as phishing, has been around for years, the targeted e-mails that address a user by name, known as social phishing, are relatively new but quickly becoming widespread. Professor Markus Jakobsson of the Center for Cybersecurity at Indiana University-Bloomington, said, "One new trend is using personal details to specifically target individuals. You can send a spoof e-mail that looks like it came from a bank, but you can just as easily make it look like it came from a friend." According to Jakobsson, cyber scammers are now harvesting contact lists from popular networking sites. They then send spoof e-mails to individuals that arrive under the names of a person's real-life friends. In a recent study, Jakobsson said he was able to acquire personal information from 19 percent of the eBay users he targeted in a single try.

Source: <http://www.newsday.com/news/local/newyork/am-spam0227.0.1026718.story?track=rss>

17. *February 25, San Francisco Chronicle (CA)* — **Stolen laptop had clients' private data, says Ernst & Young.** Financial giant Ernst & Young acknowledged Friday, February 24 that it had lost sensitive data that could be exploited by identity thieves. In a letter dated Monday, February 13, Ernst & Young warned clients that their Social Security numbers were on a laptop that was stolen from an employee's locked car. The letter didn't say how many clients were affected. Ernst & Young spokesperson Charles Perkins offered a prepared statement saying that the laptop was password protected, and appeared to have been stolen in a random criminal act. There is no indication that the lost information has been used for fraud. The laptop had no label indicating it contained sensitive information. "There are so many things that companies need to factor into their security and privacy protection measures. It's not just firewalls for the computer systems, it's the handling of backup tapes, CDs and DVDs, and paper records," said Beth Givens, director of the Privacy Rights Clearinghouse.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/02/25/BUG2IHEGCC1.DTL&hw=security+breach&sn=001&sc=1000>

18. *February 24, Federal Computer Week* — **More phishers impersonate government.** More cybercriminals are pretending they are government agencies to fool people into providing confidential information or downloading malware, security expert Alfred Huger of Symantec Security Response said. More phishing scams involve impersonating the Internal Revenue Service (IRS), especially during tax season, he said. Huger said he has seen at least 50 instances of phishers using the IRS scam. If a scam appears more than once, it means cybercriminals are making money with it, he said. Until now, phishers have concentrated on impersonating commercial organizations more than government ones, Huger said. But that is changing, he said. He expects more phishing attacks to use federal, state and local government bodies as masks for their activities.

Source: Source: <http://www.fcw.com/article92433-02-24-06-Web&RSS=yes>

[[Return to top](#)]

## **Transportation and Border Security Sector**

19.

*February 27, USA TODAY* — **Unusual headwinds prolong flights.** Unusually strong February winds at high altitudes have led to longer flight times, unscheduled pit stops, and higher costs for U.S. airlines. David Neeleman, CEO at discount carrier JetBlue, called it a "10-to-20-year event," in a speech to investors at a conference last week. The problem, which mainly has affected long distance east-to-west flights, costs his airline money by disrupting its schedule. Making matters worse, JetBlue and other airlines say, the northern and southern legs of the jet stream nearly merged, making it impossible to fly around the high head winds. Fred Johnson, of the National Oceanic and Atmospheric Administration, says the jet stream seems to be returning to its normal winter condition. When the jet stream was at its strongest, JetBlue's westbound ground speeds, normally more than 400 mph, fell to about 330 mph. Eastbound planes, with the tail wind, zoomed to 518 mph. An unplanned fuel stop adds to the costliest portions of a trip — a landing and a takeoff. A backed-up schedule adds to overtime for workers, and might require an airline to placate inconvenienced passengers with vouchers for food, lodging or future travel. US Airways, American, United, Delta, Northwest, and Continental all reported wind-driven problems.

Source: [http://www.usatoday.com/travel/flights/2006-02-26-winds-usat\\_x.htm](http://www.usatoday.com/travel/flights/2006-02-26-winds-usat_x.htm)

20. *February 27, Scotsman (Scotland)* — **UK pilots seek probe into fumes that make flight crews dizzy.** British pilots demanded an investigation on Sunday, February 26, into claims that poisonous fumes had made aircrew feel dizzy and nauseous. The move followed reports of more than 100 incidents of oil fumes inside British aircraft in the last three years and estimates that nearly 200,000 passengers a year are being exposed to them. The incidents include more than 40 in which pilots may have been partially impaired while flying. Many needed to be put on oxygen masks, while some admitted making mistakes on take-off and landing. Among events reported to the Civil Aviation Authority, a British Airways flight crew complained of stinging eyes, and a strong taste and burning in their mouths after breathing fumes during an Edinburgh-Heathrow flight last September. Sources of the problem are believed to include faulty engine seals. The most affected aircraft include the BAE-146 and Boeing 757s.

Source: <http://news.scotsman.com/uk.cfm?id=298512006>

21. *February 27, Canadian Press* — **A new idea for Canadian airport security.** The Canadian federal agency responsible for scrutinizing passengers and baggage plans to team up with the Royal Canadian Mounted Police (RCMP) to test the use of bomb-sniffing German shepherd dogs. The Canadian Air Transport Security Authority (CATSA) is negotiating terms of a possible pilot project with the RCMP and the airport authority of a major Canadian city, said CATSA spokesperson Anna-Karina Tabunar. The RCMP would be a crucial partner in the exercise, given the force's longstanding work with canines, she added. The Canada Border Services Agency already employs dogs, skilled at detecting drugs and firearms, at international airports in cities including Halifax, Quebec City, Montreal, Ottawa, Toronto, Winnipeg, Calgary, and Vancouver.

Source: <http://www.logisticsmgmt.com/index.asp?layout=articleXml&xml Id=359611680>

22. *February 27, Associated Press* — **Northwest jet makes emergency landing in Japan.** A Northwest Airlines Boeing 747 jumbo jet heading to Los Angeles from Hong Kong via Tokyo made an emergency landing in Okinawa Saturday, February 25, after smoke poured into the passenger cabin, Northwest spokesperson Masaki Takahashi said. The smoke came from an engine that had mechanical trouble, said, Takahashi.

Source: [http://www.usatoday.com/travel/flights/2006-02-27-nwa-emerge\\_ncy\\_x.htm](http://www.usatoday.com/travel/flights/2006-02-27-nwa-emerge_ncy_x.htm)

23. *February 27, USA TODAY* — **Indiana suspicious of toll road deal.** An Australian–Spanish consortium, Macquarie–Cintra, that manages roads around the world including the 7.8-mile Chicago Skyway, has offered Indiana \$3.85 billion to take up all maintenance, operations and revenue on the money-losing Indiana East–West Toll Road for 75 years. Privatizing one of the Midwest's most important roads has become a complicated issue. The concept, emerging as a trendy way for states to pay for road construction, has triggered staunch resistance. Many citizens are nervous about the prospect of transforming a 50-year-old public road into a profit-making entity and have expressed distrust toward overseas ownership. The unfolding debate serves as a test case for the growing number of states — including Texas, Virginia, Delaware, and New Jersey — that are considering similar deals. Many, like Indiana, are struggling to pay for new roads and bridges when congestion is on the rise and fuel taxes have not kept pace with expenses.

Source: [http://www.usatoday.com/news/nation/2006-02-27-indiana\\_x.htm](http://www.usatoday.com/news/nation/2006-02-27-indiana_x.htm)

24. *February 27, Associated Press* — **California airport temporarily evacuated.** About 1,000 passengers were briefly evacuated from Long Beach Airport on Monday morning, February 27, after a man ran away from a security screening, authorities said. The man was detained about an hour later a mile from the airport and was being questioned, city police Officer Juan Gomez said. The ticketed passenger passed a metal detector but federal screeners noticed his baggy clothing and decided to conduct a more intensive search, Gomez said. The man asked to use the bathroom and was escorted there but after returning and before he could be searched, he ran out a side door onto the airport tarmac, Gomez said.

Source: <http://dwb.newsobserver.com/24hour/nation/story/3202291p-119 18025c.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

25. *February 27, Agence France–Presse* — **Japanese vets arrested for hiding poultry infections.** Japanese police arrested three veterinarians and an employee of an egg farm company for allegedly hiding bird flu infections. Two veterinarians were accused of failing to report to local authorities about bird flu at farms owned by IKN Egg Farms Co. in August 2005, said a police spokesperson in Ibaraki prefecture east of Tokyo. The pair, another veterinarian and a research official of the company were also suspected of submitting false blood samples to local inspectors. Ibaraki is the prefecture most affected by the flu. The first case was found in June 2005 and since then another 40 poultry farms have seen infections, with workers killing 3.26 million birds. The virus found there was H5N2.

Source: [http://news.yahoo.com/s/afp/20060227/hl\\_afp/healthflu\\_japan\\_crime\\_060227114847;\\_ylt=AkyqWFVSuwYCeCaezEVoiiJOrgF;\\_ylu=X3oD](http://news.yahoo.com/s/afp/20060227/hl_afp/healthflu_japan_crime_060227114847;_ylt=AkyqWFVSuwYCeCaezEVoiiJOrgF;_ylu=X3oD)

26. *February 27, Associated Press* — **State brand inspection helps prevent stolen cattle and horses.** Even with microchip technology to track animals, nothing beats an old-fashioned brand, officials say. Figures compiled last year by the Animal Health and Identification Division of the Oregon Agriculture Department show the livestock industry depends on brand inspection to track herds and prevent rustling. With so many animals bought, sold, and transported across state lines, it is important to be able to track livestock that may be missing or stolen, officials say. A brand is unique to the owner and is recorded by the state in an electronic database that registers brands on cattle, horses, and some sheep.  
Source: <http://www.gazettetimes.com/articles/2006/02/27/news/oregon/state03.txt>

[[Return to top](#)]

## **Food Sector**

27. *February 23, Food Safety and Inspection Service* — **Initiative to reduce Salmonella in meat and poultry.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) Thursday, February 23, announced a comprehensive initiative to reduce the presence of Salmonella in raw meat and poultry products. The initiative will include concentrating resources at establishments with higher levels of Salmonella and changes the reporting and utilization of FSIS Salmonella verification test results. The effort is patterned after the highly successful FSIS initiative to reduce the presence of E. coli O157:H7 in ground beef. The FSIS E. coli O157:H7 initiative led to a 40 percent reduction in human illnesses associated with the pathogen. Certain serotypes of Salmonella, which are known to cause human illness, are commonly found in raw meat and poultry. Other food sources, such as produce and eggs, are also known to cause salmonellosis. Where FSIS has performed Food Safety Assessments (FSAs) in establishments that have persistently poor performance records for controlling Salmonella, there has been a dramatic reduction in the levels of Salmonella. These results have clearly demonstrated that establishments can indeed control the incidence of Salmonella in the raw products they produce. FSAs are comprehensive, systematic evaluations of a firm's food safety system performed by Enforcement, Investigation and Analysis Officers.  
Source: [http://www.fsis.usda.gov/News\\_&\\_Events/NR\\_022306\\_01/index.as.p](http://www.fsis.usda.gov/News_&_Events/NR_022306_01/index.as.p)
28. *February 23, American Phytopathological Society* — **First report of a defect of processing potatoes in Texas and Nebraska associated with a new phytoplasma.** An outbreak of a new potato disease occurred in Texas and Nebraska causing a serious defect in potato chips produced from commercial processing potatoes. The defect consists of patchy brown discoloration of chips and can be a cause for rejection of contracted potatoes by the processor. Infected potato plants exhibit symptoms of the purple top wilt syndrome similar to those of the purple top disease in processing potatoes caused by clover proliferation phytoplasma recently found in Washington and Oregon. Foliar symptoms include stunting, chlorosis, slight purple coloration of new growth, swollen nodes, proliferated axillary buds, and aerial tubers. Tuber symptoms include mild vascular discoloration and brown flecking of medullary rays. Seed potatoes from affected plants produce hair sprouts. Total nucleic acid was extracted from leaf and stolon tissue of symptomatic plants in the field and from tuber samples exhibiting the defect from commercial storages. In Texas and Nebraska, it appears that at least two distinct

phytoplasmas seem to be involved in the disease complex contributing to the defects of processed products produced from infected potatoes.

Source: <http://www.apsnet.org/pd/searchnotes/2006/PD-90-0377B.asp>

[[Return to top](#)]

## **Water Sector**

29. *February 26, KSL-TV (UT)* — **Water situation worrisome in Southern Utah.** Snow measurements in Southern Utah are so different from last year that instead of worrying about floods, this year people are worrying about drought. At a key measuring station east of Cedar City, the snow depth is less than a quarter of last year, but even worse, the water content is practically zero. Randy Julander, Snow Survey Expert: "It would take probably two storms every week from now until mid-April to catch them back up to normal. I just don't see that happening."

Source: <http://www.ksl.com/?nid=148&sid=169097>

30. *February 26, Associated Press* — **Las Vegas saves millions of gallons of water by listening for leaks.** Las Vegas's water authority has saved more than 575 million gallons of water by listening carefully for leaks with a \$2.1 million high-tech surveillance system, an official said. Over the past two years, the Las Vegas Water District has installed 8,000 listening devices beneath streets across the valley. The devices listen for the telltale sign of leaky pipes and officials say a four-person crew has been able to use the devices to detect 600 leaks that might not have been found otherwise. Patching the leaks has saved the loss of more than 575 million gallons of water, enough to supply 3,200 households for one year, the district said. Finding small leaks before they sprout into larger problems also saves time and money. Las Vegas was the first city in the country to apply the technology system wide.

Source: <http://www.lasvegassun.com/sunbin/stories/nevada/2006/feb/26 /022610734.html>

[[Return to top](#)]

## **Public Health Sector**

31. *February 27, BBC* — **Deadly bird flu spreads to Niger.** Niger has confirmed cases of the H5N1 strain of bird flu, according to the World Organization for Animal Health (OIE). Niger has a long border with Nigeria, where bird flu has killed thousands of chickens. No human cases of the H5N1 strain have yet been found in Africa but the United Nations has warned of a possible regional disaster. The H5N1 strain was found in domestic ducks near Nigeria's border, the OIE said. Nigeria's Information Minister Frank Nweke announced that the H5N1 strain had been found in two more Nigerian states, taking the total to seven -- mostly in the north and center of the country.

Source: <http://news.bbc.co.uk/1/hi/world/africa/4755042.stm>

32. *February 27, Agence France-Presse* — **Indonesia starts fourth polio immunization round.** Indonesia kicked off its fourth nationwide round of polio immunizations, hoping to bring to an end a resurgence of the crippling disease. Welfare Minister Aburizal Bakrie said that the \$24.8

million drive was targeting more than 23 million children aged under five across the country. More than 250,000 immunization posts have been set up around the country. A fifth round is scheduled in April. Polio infections have been confirmed in 304 children in Indonesia since it resurfaced in March 2005, a decade after it was believed to have been eradicated.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: [http://news.yahoo.com/s/afp/20060227/hl\\_afp/healthpolioindonesia\\_060227112005:ylt=Appen122gIxRjDKrQQ5YcRyJOrgF:ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--](http://news.yahoo.com/s/afp/20060227/hl_afp/healthpolioindonesia_060227112005:ylt=Appen122gIxRjDKrQQ5YcRyJOrgF:ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--)

33. *February 27, Reuters* — **France starts poultry vaccination as bird flu spreads.** France began vaccinating more than 300,000 geese and ducks against bird flu on Monday, February 27.

France started the vaccination campaign in the department of the Landes, in the southwest of the country, one of the areas deemed to be at risk from the spread of the virus by migratory birds. France is Europe's biggest poultry producer and has a confirmed case of H5N1 bird flu at a turkey farm in the east, the first farm in the European Union to contract the virus. The Netherlands also has plans to vaccinate some of its backyard and free-range poultry.

Source: [http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006-02-27T124808Z\\_01\\_L17684842\\_RTRUKOC\\_0\\_US-BIRDFLU.xml&archived=False](http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006-02-27T124808Z_01_L17684842_RTRUKOC_0_US-BIRDFLU.xml&archived=False)

34. *February 27, Agence France-Presse* — **World vets meet in France.** International veterinary experts gathered in Paris, France, to discuss the fight against the H5N1 strain of bird flu. Chief veterinary officers from more than 50 countries in Europe as well as Kazakhstan, Azerbaijan, Syria, and Iran started a two-day meeting at the World Organization for Animal Health (OIE) aimed at coordinating their response to the worsening epidemic. "They will be hearing country-by-country situation reports, analyzing the way the virus is spreading, and recommending coordinated measures for detection and control," said OIE spokesperson Maria Zampaglione. Experts fear that H5N1, which has killed more than 90 people, mostly in Asia, since 2003, may mutate into a form that can pass between humans, launching a pandemic that could kill millions. Human deaths have been recorded in Cambodia, China, Indonesia, Iraq, Thailand, Turkey, and Vietnam.

Source: [http://news.yahoo.com/s/afp/20060227/hl\\_afp/healthfluworld\\_0\\_60227152624](http://news.yahoo.com/s/afp/20060227/hl_afp/healthfluworld_0_60227152624)

35. *February 27, Agence France-Presse* — **Bosnia confirms first case of deadly bird flu.** Bosnia confirmed Monday, February 27, its first case of the H5N1 strain of bird flu which has been found on samples of two wild swans found dead earlier this month. The two swans had been killed in mid-February at the Plivsko Lake near the central town of Jajce.

Source: <http://www.todayonline.com/articles/103541.asp>

36. *February 25, Reuters* — **Indian Ocean virus infections climb in Mauritius.** The number of people in Mauritius infected with a mosquito-borne disease which is ravaging through the Indian Ocean region has risen to 962 from 341 the previous week, the government said on Friday, February 24. Chikungunya has been spreading through islands off the southeast coast of Africa since January, affecting more than 150,000 people in Reunion, Seychelles, and Mauritius. The Mauritian government says the situation is under control. Authorities blame the spread of the disease on heavy rains in recent months and have launched a countrywide public awareness campaign. Seychelles, which reported at least 1,000 cases at the beginning of

February, says numbers have now started to decline with the end of heavy rains.

Chikungunya information: <http://www.phac-aspc.gc.ca/msds-ftss/msds172e.html>

Source: <http://www.alertnet.org/thenews/newsdesk/L25770433.htm>

**37. *February 25, Deccan Herald (India)* — Indian village attacked by mysterious disease.**

People of the Indian village of Belagatta in Chitradurga taluk seem to be suffering from a mysterious disease. A similar situation was reported from Devasamudra village of Molakalmuru taluk, near Bellary district. People who are ailing from this disease, are reported to be suffering from symptoms of severe cold, fever, and joint pain. This strange disease has proved to be a challenge to the officials of the Health department. They are unable to diagnose it. The disease is found in different age groups. By evening, the patients start shivering from severe cold, followed by fever and joint pains. The pain is so severe that it leaves the patients crippled, unable to move around or attend to their daily chores. Also it worsens with swelling in the hands and legs of the patients. The symptoms were reported in the surrounding areas of Devasamudra village, for the last month. Now this was reported from Belagatta and the nearby areas.

Source: [http://www.deccanherald.com/deccanherald/feb252006/district1\\_715152006224.asp](http://www.deccanherald.com/deccanherald/feb252006/district1_715152006224.asp)

**38. *February 24, New Scientist* — Huge protein–interaction database could save lives.** The first large–scale analysis of how proteins interact inside our cells may help biologists identify novel gene mutations involved in human disease, researchers say. The laborious analysis, which has so far reviewed 25,000 protein interactions, suggests that important proteins do not necessarily interact with many others. To construct this "interactome", Akhilesh Pandey of the Johns Hopkins School of Medicine, and his colleagues worked with about 70 biologists in Bangalore, India. At the Institute of Bioinformatics in Bangalore the scientists survey the scientific literature, distilling findings regarding protein interactions from research papers and coding these findings into an electronic database.

Source: <http://www.newscientist.com/channel/health/dn8773.html>

[[Return to top](#)]

## **Government Sector**

**39. *February 24, Government Technology* — Near real–time "Who's in jail" database running in Kentucky.** Kentucky Lieutenant Governor Steve Pence introduced a new program on Thursday, February 23, JusticeXchange, which is now available to the state's criminal justice community. JusticeXchange is a Web portal that provides law enforcement and other criminal justice officials instant access to information about offenders held in jails throughout the state and across the country. Based on data collected automatically from local jail management systems, JusticeXchange provides near real–time current and historical information about incarcerated offenders, including biographical information, charges, photographs, and behavioral reports, all accessible through a secure Website. JusticeXchange currently tracks 100 percent of state and local jail beds in Kentucky. The system also accounts for 43 percent of all county jail beds throughout the country. Currently, data from 27 states is in JusticeXchange. Kentucky is one of at least seven states that have launched a statewide JusticeXchange system. Other states include Arkansas, New York, Washington, Utah, Texas, and Florida. JusticeXchange Website: <http://www.appriss.com/JusticeXchange.html>

[\[Return to top\]](#)

## **Emergency Services Sector**

40. *February 27, Federal Computer Week* — **Hurricane response highlighted the need to standardize digital maps.** Emergency responders dispatched to disaster scenes face one of their biggest obstacles in trying to find victims in the midst of chaos. Hurricanes, floods and bombs knock down street signs, which serve as guides for rescue workers. Global Positioning System (GPS) devices and print-on-demand maps offer rescuers navigation aids that were unavailable even a decade ago. As useful as those devices are, however, local, state and federal relief workers don't always have enough data, enough GPS devices or adequate technical understanding to use coordinate systems effectively. Some federal agencies pinpoint locations with a geospatial data standard called the National Grid. Local governments use latitude and longitude, and some states rely on their own coordinate systems. When disaster strikes, relief workers can't easily coordinate data to aid their search-and-rescue efforts. The interoperability problem came to a head after Hurricane Katrina hit. A major complication in integrating all the data is acquiring the data. Many localities are reluctant to share maps because they contain private information, while some local governments sell their data to make money.

Source: <http://www.fcw.com/article92427-02-27-06-Print>

41. *February 26, WJZ-TV (MD)* — **Maryland Transit Authority and emergency responders simulate train derailment.** Maryland Transit Authority (MTA) and MARC train emergency units were put to the test Sunday, February 26, when a simulated train derailment took place off of Key Highway in Baltimore, MD. The objective of the drill: To discover whether emergency responders fully understand the situation from dispatchers so they can properly respond. MTA officials say that special operations and emergency medical services worked well together and that a report detailing Sunday's drill will be released in the next few weeks.

Source: [http://wjz.com/local/local\\_story\\_057231101.html](http://wjz.com/local/local_story_057231101.html)

42. *February 26, Portland Press Herald (ME)* — **Maine Task Force identifies security lapses.** Maine needs better emergency radio links and backup generators at new schools to improve the state's ability to cope with a terrorist attack or other emergencies. Those are two of the recommendations of the state Task Force to Study Maine's Homeland Security Needs, which will release an interim report this week. The 11-member panel, which includes lawmakers from both major parties and public members, plans to submit legislation this week to improve the state's emergency-response system. The panel wants the state to incorporate emergency planning into school curriculums, upgrade the qualifications and emergency powers of municipal health officers and make it easier for hospitals to hire staff during emergencies. The interim report includes a long list of recommendations that call for more state and federal funding and better coordination among key state agencies. The report says the state should teach residents disaster preparation and take steps to assure that medical resources are adequate to cope with a large-scale emergency. One of the most important recommendations calls on the state to set aside at least six public-safety radio frequencies as disaster channels.

Source: [http://pressherald.maintoday.com/news/statehouse/060226home\\_land.shtml](http://pressherald.maintoday.com/news/statehouse/060226home_land.shtml)

**43. February 25, Tri-Valley Herald (CA) — California cities share disaster plans.** City officials from five California cities demonstrated the region's proactive approach toward disaster preparedness by discussing regional response plans Thursday night, February 23. The Tri-Valley Council Meeting — held at the Dougherty Station Community Center in San Ramon, CA — included representatives from the Livermore-Pleasanton Fire Department, San Ramon Valley Fire Department, Emergency Operations Center officials and other first-responders. "It is an opportunity for the communities come together and really evaluate what's being done in each of the different cities, and what we can learn from one another," Livermore-Pleasanton Fire Chief Bill Cody said. City officials seemed confident that the meeting was a first step towards being ready for disaster. "It shows we are on the same page, and there is interaction with the other cities," said Brian Lindblom, emergency preparedness coordinator for San Ramon.

Source: [http://www.insidebayarea.com/trivalleyherald/localnews/ci\\_3546113](http://www.insidebayarea.com/trivalleyherald/localnews/ci_3546113)

**44. February 24, Associated Press — FEMA: New Madrid earthquake preparedness is agency priority.** Preparing for a catastrophic earthquake along the New Madrid fault is a priority, Federal Emergency Management Agency (FEMA) official, Michel Pawlowski, said Friday, February 24, before a congressional field hearing on government readiness to handle natural disasters. The New Madrid Seismic zone lies within the central Mississippi Valley, extending from northeast Arkansas, through southeast Missouri, western Tennessee, western Kentucky to southern Illinois. Pawlowski told a congressional committee that FEMA has "significant concerns" for the potential of a catastrophic earthquake equal in magnitude to those that struck parts of the Mississippi River Valley in 1811–1812, and again in 1895. Even a magnitude 7 earthquake would destroy more than 60 percent of buildings in St. Louis, MO, and Memphis, TN, because most buildings predate building requirements aimed at resisting the shock, officials estimate. Also, FEMA officials are worried about how quickly they could enter the affected area after an earthquake because many roads, bridges, and approaches are not expected to withstand a high-magnitude earthquake, Pawlowski said. FEMA expects to have a regional response plan in place by June 2007.

Source: [http://www.nctimes.com/articles/2006/02/25/news/nation/16\\_58\\_312\\_24\\_06.txt](http://www.nctimes.com/articles/2006/02/25/news/nation/16_58_312_24_06.txt)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

**45. February 27, Internet News — Rural America closing broadband gap.** The gap between rural and non-rural home broadband adoption, though still substantial, is narrowing. According to a new study by the Pew Internet & American Life Project, 24 percent of adult rural Americans went online with a high-speed connection by end of 2005, compared to 39 percent of home broadband users in urban and suburban areas. For overall rural Internet use, the penetration rate for adult rural Americans lagged the rest of the country by eight percentage points at the end of 2005. This is about half the gap that existed at the end of 2003. "Growth in rural broadband adoption has been fast relative to urban and suburban areas in the past two years," the Pew report states.

Rural Broadband Internet Use study:

[http://www.pewinternet.org/pdfs/PIP\\_Rural\\_Broadband.pdf](http://www.pewinternet.org/pdfs/PIP_Rural_Broadband.pdf)

Source: <http://www.internetnews.com/infra/article.php/3587711>

46. *February 25, Ars Technica* — **Malware moves up, goes commercial.** Engineers at Panda Software uncovered evidence last week that led them to a Website touting custom-built viruses for sale. For the price of \$990, a user gets his or her own pet Trojan horse, complete with tech support. If the file is discovered — as this current model was — the designer provides a guarantee to alter it so that it may continue to avoid detection in the face of updated antivirus software. The Trojan goes by the moniker Trj/Briz.A, and scans the user's hard drive for information that could be used for financial and identity data. It then sends that information to an attacker working behind the scenes. Additional features include the ability to gather IP addresses and in some cases, the physical location of infected computers. It can also modify the machine to prevent access to Websites devoted to antivirus products. The file that causes the Trj/Briz.A infection is called "iexplore.exe." It uses this name to pass itself off as Internet Explorer.

Source: <http://arstechnica.com/news.ars/post/20060225-6264.html>

47. *February 24, CNET News* — **Security experts: Threats to cell phones are likely to increase.** Programs that fight viruses have become a necessary evil on Windows PCs. Now the antivirus industry is turning its attention to mobile phones — but it's running into reluctance from cell service providers, who aren't so sure that the handset is the best place to handle security. Verizon Wireless doesn't see a need for its customers to install antivirus software on cell phones. "At this point, that is absolutely not required by individual customers," spokesperson Jeffrey Nelson said. But makers of security software are eager to get their products onto handsets, a huge potential market. About 812 million mobile terminals — such as cell phones and smart phones — were sold in 2005, according to market researcher Gartner. That compares with an estimated 219 million PCs in the same period. The market research firm expects annual mobile device shipments to exceed one billion units for the first time in 2008. While the number of threats to cell phones is low, security experts and analysts agree that situation is likely to change. Gartner suggests a widespread attack could surface by the end of next year.

Source: [http://news.com.com/Is+your+cell+phone+due+for+an+antivirus+shot/2100-7349\\_3-6042745.html](http://news.com.com/Is+your+cell+phone+due+for+an+antivirus+shot/2100-7349_3-6042745.html)

48. *February 23, Network World* — **Researchers claim advances in using fingerprints to secure networks.** University of Buffalo, NY, researchers say they have found a way to improve security of wireless handheld devices and Websites. The research specifies how big a keypad sensor needs to be and how big a fingerprint image should be, as a key shortcoming of biometric systems now is that sensors often only can take partial fingerprints, says Venu Govindaraju, a University of Buffalo professor of computer science and engineering, and director of the school's Center for Unified Biometrics and Sensors (CUBS). The researchers' work has been published in the journal Pattern Recognition.

Source: <http://www.networkworld.com/news/2006/022706-fingerprint-security.html>

## Internet Alert Dashboard

## DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US-CERT Vulnerability Note:

VU#999708 – Apple Safari may automatically execute arbitrary shell commands

Although there is limited information on how to fully defend against this exploit, US-CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser document.

### **Public Exploit Code for Buffer Overflow Vulnerability in Microsoft Windows Media Player Plug-in for Non-IE Browsers**

US-CERT is aware of publicly available exploit code for a buffer overflow vulnerability in Windows Media Player plug-in for browsers other than Internet Explorer (IE). For more information can be found in the following US-CERT Vulnerability Note:

VU#692060 – Microsoft Windows Media Player plug-in buffer overflow  
<http://www.kb.cert.org/vuls/id/692060>

US-CERT urges users to apply appropriate updates and review the workarounds listed in Microsoft Security Bulletin MS06-006 to mitigate this vulnerability.  
<http://www.microsoft.com/technet/security/Bulletin/MS06-006.msp>

## Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 25 (smtp), 5435 (dtl), 139 (netbios-ssn), 2798 (tmesis-upshot), 55556 (----), 41170 (----), 29398 (----) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[\[Return to top\]](#)

## **General Sector**

Nothing to report.

[\[Return to top\]](#)

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:  
<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644.
Subscription and Distribution Information:	Send mail to <a href="mailto:dhsdailyadmin@mail.dhs.osis.gov">dhsdailyadmin@mail.dhs.osis.gov</a> or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.